Application of Probabilistic Risk Assessment (PRA) During Conceptual Design for the NASA Orbital Space Plane (OSP)

Presented to PRAXI-5
Cleveland, OH
October 28-29, 2004

Based on a publication by:
James Stott and Dr. Yohon Lo of
Hernandez Engineering at Marshall Space Flight Center

Dr. Fayssal Safie and James Rogers of
NASA - Marshall Space Flight Center

Introduction – Why do we do PRA?

- To estimate risks and associated uncertainties of low frequency but high consequence events

- As part of Continuous Risk Management to support risk-based decision making: Upgrades and Trades
  - For a mature system: "to support decision making on risk acceptability, and on choices among options for risk reduction"*
  - For a system under development: "to guide trade-offs between safety, reliability, cost, performance, and other tradable resources"*

- This presentation talks about one way that PRA can be used in the design phase of a complex, highly visible system

* Excerpt from M. Greenfield. NASA HQ. Risk Management Tools. May 2, 2000 LaRC presentation

What was OSP?

- The Orbital Space Plane Program was initiated to provide assured access to and from the International Space Station (ISS)
  - ISS Crew Rotation via Crew Transfer Vehicle (CTV)
  - Evacuation via Crew Rescue Vehicle (CRV)
- Competitive contractor teams
- Multiple vehicle concepts
- To be launched on top of an existing Expendable Launch Vehicle (Atlas V and Delta IV)
- CRV was scheduled to be online by 2008, CTV by 2012
- OSP Program was superseded by restructuring to support the President's new space vision in January 2004

Atlas V-H   Delta IV-H

Hernandez Engineering Inc.
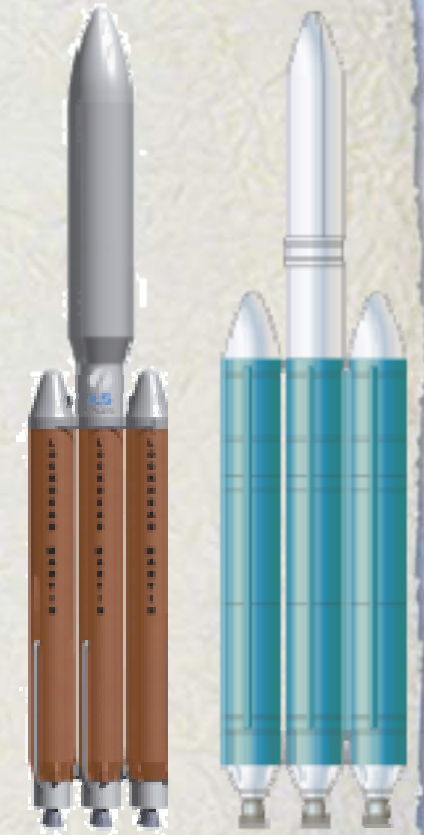
OSP Goals

- Significant improvements in crew safety:
  - Crew Rescue Vehicle (Compared to Soyuz Reentry)
    - Objective — 1/800 with 80% confidence
    - Minimum Threshold — 1/800 with 50% confidence
  - Crew Transfer Vehicle (Compared to Shuttle Ascent & Reentry)
    - Objective — 1/400 with 80% confidence
    - Minimum Threshold — 1/400 with 50% confidence
- Availability requirement (On-orbit)
  - Crew Rescue Vehicle
    - Objective — 95% with 90% confidence
    - Minimum Threshold — 95% with 50% confidence

Integrated RMS Approach

- What is an Integrated Reliability, Maintainability, and Supportability approach to PRA?
  - 2GRLV "Lesson Learned"
  - Integrated RMS approach to the PRA incorporated input from Reliability, Maintainability, and Integrated Logistics Support (ILS) Working Groups.

- NASA is beginning to implement an integrated RMS approach for new programs
  - OSP was the first space flight system that utilizes PRA in every step of its design process in conjunction with other traditional engineering disciplines

Hernandez Engineering Inc.

OSP PRA Evolution

- ISAT (Integrated System Analysis Team)
  - Technology investigation
  - Initiated during Second Generation Reusable Launch Vehicle Program
- RAC (Requirements Analysis Cycle)
  - Evaluate Level 1 and Level 2 OSP Requirements
  - Perform system level trade studies
  - PRA approach with integrated ISAT results.
- NASA OSP PRA
  - Based on the most feasible design from RAC and modeled CTV mission profile.
- OSP Prime contractors PRA
  - NASA "Guided" Groundrules and Assumptions for consistent analysis

Hernandez
Engineering Inc.

NASA OSP PRA Process

- NASA OSP PRA was a NASA wide and NASA led team effort with NASA MSFC S&MA / HEI as the lead with members from HQ, JSC, KSC, LaRC, SAIC & Futron

- Established ground rules and assumptions up to SDR, such as:
  - Modeling of Loss of Crew and Loss of Mission started from Crew Ingress to Crew Egress
  - Launch on a Atlas V
  - OSP remains on station for 180 days

- Created typical Mission Regimes and associated Mission Event Trees identifying the major operational and vehicle states
  - Such as: Ascent, Orbit, Docking, ISS Mated, Re-Entry/Landing
  - Abort scenarios are identified where appropriate

- Constructed fault trees down to system level
  - Use of existing PRA (Shuttle, ISS, Soyuz, ELV) results when possible

- Determined that Program Level I safety requirement can be met

Contractor OSP PRA Process

1. OSP Program redirected the NASA OSP PRA WG to stop development of NASA OSP PRA and to support the Contractor PRA effort

2. NASA OSP PRA WG sanitized the existing NASA OSP PRA models and results for the contractors
   - Generic top level event tree models (non-design specific)
   - Via contractual requirement document (OSP PRA Plan)
   - Purpose
     - Ensure consistency among the contractors
     - Test problem for contractors to demonstrate its architecture's capabilities

3. Contractors to modify and to expand the generic top level model to meet its design capabilities

4. Weekly telecons with All Contractors and NASA WGs
   - Allow contractors to ask questions
   - Unified voice / recommendations from NASA to Contractors

5. Program Cancellation …

Summary of OSP PRA Process

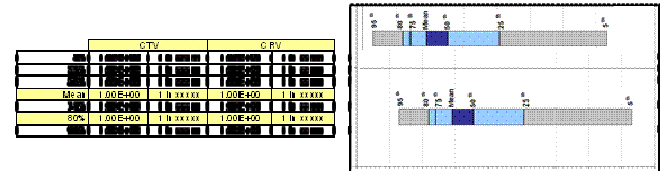| EELV Data and EELV PRA Results	Shuttle, Soyuz, ISS PRA Results	Shuttle, Soyuz, ISS PRA Results	Engineering Analysis, Judgment and Generic Data

Ascent Model

On-Orbit Model

Descent Model
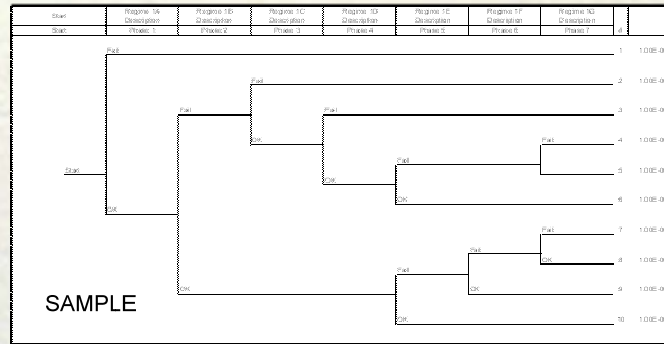
SAMPLE

OSP PRA Model in SAPHIRE

MS Excel: Results Post Process Calculations

Numerical and Graphical Outputs

SAMPLE

SAMPLE

Hernandez Engineering Inc.

Conclusions

- PRA is a valuable tool to perform system level trade studies on conceptual vehicles
    - By integrating PRA in the design process, it allows for a systematic approach in performing the various trade studies
    - Provides basis for risk based decision making
- To get the most benefits from PRA in the design process
    - Maintain close interactions between PRA and all program teams to improve state of knowledge
    - Formulate ground rules early and maintain proper documentation to ensure consistency and traceability

Hernandez
Engineering Inc.

Backup

Hernandez
Engineering Inc.

Typical OSP Operating Regimes

Orbital Insertion

Mated Ops with ISS Regime 6

~ 460 km Regime 5 ends

~460 km Regime 7

~230 km Regime 4 ends, abort to land capability – Abort to Orbit begins

~150 km, ascent TPS limit Regime 3 ends

~ 120 km, Re-entry Regime 8

EELV Failure Escape Scenario (Contained or Uncontained):
- **OSP separation**
- **Stabilize OSP**
- **OSP lands**

Max q,

~80 km strap-on CBC jettison Regime 2 ends

~1 km, Regime 1 ends

Minimum Parachute Altitude

Hernandez Engineering Inc.